Subalgebra lattices, simplicity and rigidity

VÁCLAV KOUBEK*

Let A be a universal algebra and let Con (A), Sub (A), End (A), Aut (A) denote the lattice of all congruences of A, the lattice of all subalgebras of A, the endomorphism monoid of A, and the automorphism group of A, respectively. It is well known that Con (A) and Sub (A) can be arbitrary algebraic lattices (see [5] and [2], or [4]), End (A) can be an arbitrary monoid (see [1]). W. A. LAMPE [8] proved the independence of Con (A), Sub (A) and Aut (A) — his construction represents each pair of non-trivial algebraic lattices and an arbitrary group as Sub (A), Con (A) and Aut (A) of a finitary algebra A. SAUER and STONE [9] characterize lattices L of subsets of a given set X and transformation monoids M on X for which there is an algebra A on X with $L=\mathrm{Sub}(A)$, $M=\mathrm{End}(A)$. This is an example of a concrete characterization, while the other results represent the lattices and/or groups up to an isomorphism of the respective structures.

The relationship between the lattice of subalgebras and automorphism groups of subalgebras was studied in [3] and the characterization for a special case was given. A concrete version of this problem was solved in [6]. The aim of this paper is to continue in these considerations — we characterize pairs (L, Δ) where L is an algebraic lattice and Δ is a finitary type such that there is an algebra A of type Δ with $\mathrm{Sub}(A)\cong L$ and each subalgebra of A (including A) is rigid and simple (an algebra A is *rigid* if End (A) is trivial, and it is *simple* if Con (A) is the two-element lattice).

The method of the presented proof is based on a construction given in [7]: for a given type Δ, it shows how large algebras of type Δ exist in which every subalgebra is rigid. We strenghten this result — we show that for a given non-unary type Δ and for a given cardinal α if there is an algebra A of type Δ with power $\geqq\alpha$ such that each of its subalgebras is rigid then there is an algebra B of type Δ with power $\geqq\alpha$ such that each of its subalgebras is rigid and simple.

Received October 6, 1982.

* The support of NSERC is gratefully acknowledged.

The basic algebraic notions can be found in [4], in particular, a type Δ is *finitary* if all operation symbols in Δ have finite arities, it is *non-unary (infinitary)* if there is an operation symbol in Δ with arity >1 (infinite arity). Denote by $|\Delta|$ the number of operation symbols in Δ. We add to the class Card of all cardinals a new largest element c (i.e. $c>\alpha$ for each cardinal α).

We recall some combinatorial notions given in [7]. For a cardinal α, a pair (X, φ) is called an *α-set pair* if X is a well-ordered set and φ is a mapping from the set of all finite subsets of X into a set Y with cardinality α. A one-to-one increasing sequence $\{x_0, x_1, \ldots\}$ of elements of X (with respect to the well-ordering of X) is called *good* (w.r.t. (X, φ)) if for every finite subset A of $\{x_0, x_1, \ldots\}$ and for every natural number n, $\varphi(A)=\varphi(\{x_{i+n};\ x_i \in A\})$. Let $\mathrm{Set}(\alpha)$ be the smallest cardinal such that each α-set pair (X, φ) with the power of X greater than or equal to $\mathrm{Set}(\alpha)$ has a good sequence; if such a cardinal does not exist put $\mathrm{Set}(\alpha)=c$. We prove:

Theorem 1. *If Δ is a finitary non-unary type, set $\alpha=\max\{2^{|\Delta|}, 2^{\aleph_0}\}$. The following are then equivalent for any cardinal β:*

(a) *β is smaller than* $\mathrm{Set}(\alpha)$;

(b) *there is an algebra (A, F) of type Δ such that each of its subalgebras is rigid and* $\mathrm{card}\, A \geqq \beta$;

(c) *there is an algebra (A, F) of type Δ such that each of its subalgebras is rigid and simple and* $\mathrm{card}\, A \geqq \beta$.

In [7] the equivalence of (a) with (b) was proved. Clearly, (c)$\Rightarrow$(b) and we are to prove (a)$\Rightarrow$(c). Moreover, as in [7] from this proof we obtain:

Corollary 2. *If Δ is an infinitary type then for each cardinal α there is an algebra (A, F) of type Δ such that each of its subalgebras is rigid and simple and* $\mathrm{card}\, A \geqq \alpha$.

For an algebraic lattice L put $c(L)=\sup\{\varkappa;$ there is a compact element c of L with $\varkappa=\mathrm{card}\{d\in L;\ d$ is compact, $d<c\}\}$, $d(L)=\min\{\alpha;\ \mathrm{Set}(\alpha)>\mathrm{card}\, L\}$ (In [7] it was proved that $\mathrm{Set}(\alpha)$ is a strongly inaccessible cardinal thus $\mathrm{Set}(\alpha)>\mathrm{card}\, L$ iff $\mathrm{Set}(\alpha)>\mathrm{card}\{c\in L;\ c$ is compact$\}$.) We prove the following:

Theorem 3. *For a given algebraic lattice L and for a given finitary non-unary type Δ there is an algebra A of type Δ such that*

(a) $\mathrm{Sub}(A)\cong L$;

(b) *each subalgebra of A is rigid and simple*

if and only if $2^\alpha>d(L)$, $\alpha\geqq c(L)$ *where* $\alpha=\max\{|\Delta|, \aleph_0\}$.

Let m be a regular cardinal. We recall that a complete lattice L is called m-algebraic (see [4]) if every $x\in L$ is a join of m-compact elements of L (an element x of L is m-compact if $x\leqq\bigvee M$ for a subset M of L only if there is a subset N of M

of cardinality less than m with $x \leqq \bigvee N$). An algebraic lattice is thus an $\aleph_0$-algebraic lattice. Put $c_m(L) = \sup\{\varkappa;$ there is an m-compact element c of L such that $\varkappa = \operatorname{card}\{d \in L;\ d$ is m-compact, $d < c\}\}$. For a type Δ denote $\sup \Delta = \sup\{\alpha^+;$ there is an operation symbol in Δ with the arity $\alpha\}$ (as usual, α^+ is the cardinal successor of α). Clearly, Δ is finitary iff $\sup \Delta \leqq \aleph_0$. It is well known that for each m-algebraic lattice L there are a type Δ with $\sup \Delta \leqq m$ and an algebra A of type Δ with $\operatorname{Sub}(A) \cong L$ (see [4]). We prove the following modification of Theorem 3:

Theorem 4. *Let m be a regular cardinal, $m > \aleph_0$. Then for a given m-algebraic lattice and for a given type Δ there is an algebra A of type Δ such that*

(a) $\operatorname{Sub}(A) \cong L$;

(b) *each subalgebra of A is rigid and simple*

if and only if $\sup \Delta \geqq m$ *and* $c_m(L) \leqq |\Delta| \cdot 2^{n\alpha}$ *for some* $n < m$, $\alpha < \sup \Delta$.

I wish to acknowledge helpful discussions with J. Sichler.

To prove the theorems we need some technical notions and claims. Let $\mathbf{N}$ denote the set of all natural numbers. If (A, F) is a partial algebra of type Δ then (A', F) is called a *subalgebra* of (A, F) if $A' \subset A$ and for $f \in F$, if $f(x_1, \dots, x_n)$ is defined in (A, F) and $x_1, x_2, \dots, x_n \in A'$ then $f(x_1, x_2, \dots, x_n) \in A'$. An equivalence θ on A is called a *congruence* of (A, F) if for each $f \in F$ such that $f(x_1, x_2, \dots, x_n)$, $f(y_1, y_2, \dots, y_n)$ are defined and $x_i \theta y_i$ for each $i = 1, 2, \dots, n$ we have $f(x_1, x_2, \dots, x_n)\, \theta\, f(y_1, y_2, \dots, y_n)$. An algebra (A, G) of type Δ is called an *extension algebra* of (A, F) if the identity map is a homomorphism from (A, F) to (A, G).

A partial algebra (A, F) is called *strongly rigid (strongly simple)* if for every extension algebra (A, G) the identity map of A is the only homomorphism from (A, F) to (A, G) ((A, G) has only two congruences — trivial and total, respectively). A pair of partial algebras (A, F), (B, G) is called *strongly mutually rigid* if there is no homomorphism from (A, F), or (B, G), to any extension algebra of (B, G), or (A, F) respectively. The following proposition gives a reason for these definitions:

Proposition 5. *Let (A, F) be a partial algebra whose subalgebras are strongly rigid and strongly simple. Then each subalgebra of any extension algebra of (A, F) is rigid and simple.*

Proof is obvious.

The following lemma enables us to reduce the type Δ for which we shall prove Theorems 1 and 3.

Lemma 6. *Let $\Delta' = \{\eta_i;\ i \in I \cup \{0\}\}$ be a finitary type such that η_0 has arity greater than 1, let $\Delta = \{\sigma\} \cup \{\tau_i;\ i \in I\}$ be a type such that σ is binary and τ_i is nullary for every $i \in I$. If Theorem 1 or Theorem 3 holds for Δ then it also holds for Δ'.*

Proof. Since $\max\{2^{|\Delta|}, 2^{\aleph_0}\}=\max\{2^{|\Delta'|}, 2^{\aleph_0}\}$, (a) of Theorem 1 holds for Δ iff it holds for Δ'. Moreover, each algebra of type Δ can be represented as an algebra of type Δ' such that homomorphisms do not change. Hence we get the required assertions.

In what follows we assume that a type $\Delta=\{\sigma\}\cup\{\tau_i;\ i\in I\}$ is given such that σ is binary and τ_i is nullary for every $i\in I$. Denote by v the derived unary operation symbol, $v(x)=\sigma(x, x)$.

Choose a one-to-one mapping ζ from the set of all pairs (n, m) of positive integers, $n<m$, to N with $\zeta(n, m)>n+m$. Let $\{p_n;\ n\in \mathrm{N}\}$ be a one-to-one increasing sequence of positive integers such that $p_0=1$ and if $q=\zeta(n, m)$ then $p_q=p^k+p_{q-m+n}$ for some $k\in\mathrm{N}$, $k>0$ and a prime $p>m-n$. Lemma 8 below is a modification of a well known statement.

Construction 7. Let (A, F) be an algebra of type Δ such that $A=I\times\mathrm{N}$ and

(1) $$\tau_i(0) = (i, 0) \quad \text{for each} \quad i\in I,$$

(2) $$\sigma((i, 0), (i, n)) = (i, n+1) \quad \text{for each} \quad i\in I, \quad n\in\mathrm{N},$$

(3) $$\sigma((i, n), (i, n)) = (i, p_n) \quad \text{for each} \quad i\in I, \quad n\in\mathrm{N},$$

(4) $$\sigma((i, 2n), (i, 1)) = (i, 0) \quad \text{for each} \quad i\in I, \quad n\in\mathrm{N}, \quad n>0,$$

(5) $$\sigma((i, 2n+1), (i, 1)) = (i, 1) \quad \text{for each} \quad i\in I, \quad n\in\mathrm{N}, \quad n>0,$$

(6) $$\sigma((i, 0), (j, n)) = (i, n) \quad \text{for each} \quad i,j\in I, \quad i\neq j, \quad n\in\mathrm{N},$$

(7) $$\sigma((i, 1), (j, 0)) = (j, 0) \quad \text{for each} \quad i,j\in I, \quad i\neq j,$$

(8) the other values of σ are arbitrary.

Lemma 8. *The algebra (A, F) is simple, is generated by* $\emptyset$, $\operatorname{card} A=\max\{|\Delta|, \aleph_0\}$ *and $v^n(a)\neq a$ for each $a\in A$, $n\in\mathrm{N}$, $n>0$.*

Proof. Clearly, $\operatorname{card} A=\max\{|\Delta|, \aleph_0\}$. By (1) and (2), (A, F) is generated by $\emptyset$, by (2) and (3) $v^n(a)\neq a$ for each $a\in A$, $n\in\mathrm{N}$, $n>0$. Let θ be a non-trivial congruence on (A, F). If $(i, n)\,\theta\,(j, m)$ and $(i, n)\neq(j, m)$ then for $i\neq j$, $n\leq m$ get $(j, n)=\sigma((j, 0), (i, n))\;\theta\;\sigma((j, 0), (j, m))=(j, m+1)$. Therefore we may assume that for an $i\in I$, $(i, n)\,\theta\,(i, m)$, $n<m$, $n, m\in\mathrm{N}$. By (2) we get $(i, n+k)\,\theta\,(i, m+k)$ for each $k\in\mathrm{N}$, by (3), $(i, p_{n+k})\,\theta\,(i, p_{m+k})$. If $m+k=\zeta(n, m)$ then $m-n$ and $p_{m+k}-p_{n+k}=p^q$ are relatively prime because $p>m-n$ is a prime. If we combine these facts we see that $(i, q)\,\theta\,(i, q+1)$ for a sufficiently large $q\in\mathrm{N}$. If we use (2,) (4) and (5) we get $(i, 0)\,\theta\,(i, 1)$ and thus $(i, q)\,\theta\,(i, r)$ for each $q, r\in\mathrm{N}$ by (2). By (6), this holds for each $i\in I$ and from (7) we get $(i, 0)\,\theta\,(j, 0)$ for each $i, j\in I$. Thus $(i, q)\,\theta$ $\theta\,(j, r)$ for each quadruple $i, j\in I$, $q, r\in\mathrm{N}$; thus θ is total.

Construction 9. For every positive integer i a partial algebra (A_i, F_i) of type Δ will be constructed as follows: Let (A, F) be an algebra from Construction 7. Denote by A' a copy of the set A, for $a\in A$ we shall denote by a' the corresponding element in A'. Set $A_i=A\cup A'\cup \mathbf{N}$ (assume that A, A' and $\mathbf{N}$ are pairwise disjoint) and let F_i be an extension of F such that

(9) $\sigma(0, n)=n+1$ for each $n\in \mathbf{N}$,

(10) $\sigma(n+1, n)=0$ for each $n\in \mathbf{N}$,

(11) $\sigma(n, n)=n+1$ for $n\in \mathbf{N}$, $n<i$, $\sigma(n, n)=0$ for $n\geqq i$,

(12) $\sigma(a', a')=1$ for each $a\in A$,

(13) $\sigma(0, a)=a'$ for each $a\in A$,

(14) $\sigma(0, a')=a$ for each $a\in A$,

(15) $\sigma(2, a)=0$ for each $a\in A$,

(16) $\sigma(2, a')=1$ for each $a\in A$,

(17) $\sigma(a', b')=0$ for each $a, b\in A$, $a\neq b$,

(18) $\sigma(2, 2n)=0$ for each $n\in \mathbf{N}$, $n>2$,

(19) $\sigma(2, 2n+1)=1$ for each $n\in \mathbf{N}$, $n>2$,

(20) $\sigma(1, n)=p_n$ for each $n\in \mathbf{N}$, $n>2$.

Lemma 10. *For each positive integer i, (A_i, F_i) satisfies:*

(a) *the operation v is a total operation and it has exactly one cycle which has length $i+1$, this cycle is on the set $\{0, 1, \dots, i\}=v(A'\cup \mathbf{N})$;*

(b) *(A_i, F_i) is strongly rigid;*

(c) *(A_i, F_i) is strongly simple;*

(d) *if $i\neq j\in \mathbf{N}$ then (A_i, F_i) and (A_j, F_j) are strongly mutually rigid;*

(e) *if (B, G) is a proper subalgebra of (A_i, F_i) then $(B, G)=(A, F)$;*

(f) *there are $\max\{|\Delta|, \aleph_0\}$ pairs $x, y\in A$ such that $\sigma(x, y)$ is not defined.*

Proof. (a) follows from (9), (11), (12) and from Lemma 8 ((A, F) is a total algebra). By a routine calculation from (9), (11), (12) and (13) we get (e). If $a, b, \in A$ then $\sigma(a, b')$ is not defined and (f) follows from Lemma 8. To verify (c), let (A_i, G) be an extension algebra of (A_i, F_i) and let θ be a non-trivial congruence on (A_i, G). The first task is to show that $0\theta 1$. The proof is divided into six steps:

(i) If $a, b\in A$, then $a\theta b$ iff $a'\theta b'$.

Indeed, this follows immediately from (13) and (14).

(ii) If $a, b \in A$, $a \neq b$, then $a'\theta b'$ implies $0\theta 1$.

Indeed, if we apply (12) and (17), then $a'\theta b'$ implies $0=\sigma(a', b')\,\theta\,\sigma(b', b')=1$.

(iii) If for $a\in A$, $n\in \mathrm{N}$, $a\theta n$, then $a'\,\theta\, n+1$.

By (9) and (13) we get $a'=\sigma(0, a)\,\theta\,\sigma(0, n)=n+1$.

(iv) If for $a\in A$, $n\in\mathrm{N}$ we have $a'\theta n$ then $0\,\theta\, 1$.

From (9), (13) and (14) we obtain $a'\,\theta\, n+2$; thus we can assume that $n>i$, in which case $1=\sigma(a', a')\,\theta\,\sigma(n, n)=0$.

(v) If $a, b, \in A$ such that $a\theta b'$ then $0\theta 1$.

$0=\sigma(2, a)\,\theta\,\sigma(2, b')=1$ follows by (15) and (16).

(vi) If $n, m\in\mathrm{N}$, $n\neq m$ then $n\theta m$ implies $0\theta 1$.

If $n\theta m$ then by (9) $n+k\,\theta\, m+k$ for each $k\in\mathrm{N}$, and if $2<n<m$ then $p_{n+k}\theta p_{m+k}$ for each $k\in\mathrm{N}$ by (20). If $k+m=\zeta(n, m)$ then $p_{m+k}-p_{n+k}=p^q$ for some $q\in\mathrm{N}$, $q\geqq 1$ and some prime $p>m-n$. Therefore $m-n$ and $p_{m+k}-p_{n+k}$ are relatively prime. Hence $q\,\theta\, q+1$ for some sufficiently large $q\in\mathrm{N}$, by a property of additive semigroups of natural numbers. Then by (18) and (19) we get $0\theta 1$.

Now we show that θ is total.

(vii) If $0\theta 1$ then $n\theta m$ for each $n, m\in\mathrm{N}$

follows immediately from (9).

(viii) If $0\theta 1$ then for each $a\in A$, $a\theta 0\theta a'$.

If $0\theta 1$ then $0\theta 2$ and by (13) and (15) $a'\theta 0$; by (14) and (16) $a\theta 1$.

Hence we conclude that (A_i, F_i) is strongly simple.

Next we prove (b). Let (A_i, G) be an extension algebra and $f\colon (A_i, F_i)\to(A_i, G)$ be a homomorphism. From (a) we see that $f(0)\in\{0, 1, \dots, i\}$. Hence $f(1)=f(\sigma(0, 0))= =\sigma(f(0), f(0))=f(0)+1$ if $f(0)\neq i$, and $f(1)=0$ if $f(0)=i$. If $f(0)=i$ then $f(0)= =f(\sigma(1, 0))=\sigma(f(1), f(0))=\sigma(0, f(0))=f(0)+1$, a contradiction. If $f(0)\neq i$ then $f(0)=f(\sigma(1, 0))=\sigma(f(1), f(0))=\sigma(f(0)+1, f(0))=0$. By (e) we obtain that $f=\mathrm{id}$ because $\{x; f(x)=x\}$ is a subalgebra of (A_i, F_i) containing 0.

To prove (d) consider an extension algebra (A_j, G) of (A_j, F_j) and a homomorphism $f\colon (A_i, F_i)\to(A_j, G)$. By (a) we get that $j\leqq i$; if $j<i$ then $\operatorname{Ker} f$ is a non-trivial congruence on (A_i, F_i), thus by (c) $\operatorname{Ker} f$ is the total congruence and f is constant. This contradicts (a).

Construction 11. Let $(X, \leqq)$ be a well-ordered set. We shall construct a partial algebra $(A(X), F(X))$ of type Δ. For every finite subset Y of X we take one copy of A, we denote it by $A(Y)$, and if $Y\neq\emptyset$ we take one copy of N, we denote it by $\mathrm{N}(Y)$. Set $A(X)=\bigcup\{A(Y); Y\subset X, Y$ is finite$\}\cup\bigcup\{\mathrm{N}(Y); Y\subset X, Y\neq\emptyset, Y$ is finite$\}$. For a finite $Y\subset X$ and for $x\in A\cup\mathrm{N}$, let $x(Y)$ be the corresponding point in $A(Y)\cup\mathrm{N}(Y)$. Further, define $\tau_Y\colon A_n\to A(X)$ (where $n=\operatorname{card} Y$) as follows: $\tau_Y(a)=a(\emptyset)$ for $a\in A$, $\tau_Y(a')=a(Y)$ for $a\in A$, $\tau_Y(n)=n(Y)$ for $n\in\mathrm{N}$. Denote by $F'(X)$ a set of partial operations on $A(X)$ of type Δ injectively generated by τ_Y, $Y\subset X$,

$\emptyset \neq Y$, Y is finite (i.e. $(A(X), F'(X))$ is the smallest partial algebra of type Δ such that $\tau_Y\colon (A_n, F_n) \to (A(X), F'(X))$ is a homomorphism for every finite non-empty subset Y of X). We shall identify $x \in X$ with $0(\{x\}) \in A(X)$, thus $X \subset A(X)$. For each pair of positive integers k, q choose a one-to-one mapping $\psi_{k,q}$ from the set of all pairs of natural numbers (n, m) with $n \leqq k, m \leqq q$ into $\mathbf{N}$ such that $\psi_{k,q} = \psi_{q,k}$. Let $(A(X), F(X))$ be the smallest extension (partial) algebra of $(A(X), F'(X))$ satisfying

(21) $\sigma(x, y) = \max\{x, y\}$ for each $x, y \in Y$, $x \neq y$,

(22) $\sigma(n(Y), m(Z)) = s(Y \cup Z)$ for each pair of distinct nonempty finite subsets Y, Z of X, for each pair $n, m \in \mathbf{N}$ with $n \leqq \operatorname{card} Y$, $m \leqq \operatorname{card} Z$ and either $n \neq 0$ or $m \neq 0$, where $s = \psi_{\operatorname{card} Y, \operatorname{card} Z}(n, m)$,

(23) $\sigma(3(Y), (4+k)(Y)) = y_k$ for each finite non-empty subset Y of X, for each $k < \operatorname{card} Y$, where y_k is the k-th point of Y.

By the choice of $\psi_{k,q}$ we get $\sigma(n(Y), m(Z)) = \sigma(m(Z), n(Y))$ in (22).

Proposition 12. *For every well-ordered set $(X, \leqq)$, $(A(X), F(X))$ fulfils:*

(a) *for every finite subset Y of X there are* $\max\{|\Delta|, \aleph_0\}$ *pairs x, y in A_n such that $\sigma(\tau_Y(x), \tau_Y(y))$ is not defined;*

(b) *for each subset Y of X, the subalgebra of $(A(X), F(X))$ generated by Y is on the set $\bigcup\{\operatorname{Im} \tau_Z;\ \emptyset \neq Z \subset Y,\ Z$ is finite$\}$;*

(c) *for every extension algebra $(A(X), G)$ of $(A(X), F(X))$, each subalgebra (B, G') of $(A(X), G)$ is generated by $B \cap X$;*

(d) *the lattice of subalgebras of $(A(X), F(X))$ is isomorphic to the lattice of all subsets of X;*

(e) *each subalgebra of $(A(X), F(X))$ is strongly simple;*

(f) *for every pair of finite subsets Y, Z of X with* $\operatorname{card} Y = \operatorname{card} Z$ *there is an isomorphism between the subalgebras of $(A(X), F(X))$ generated by Y and Z;*

(g) *for every extension algebra $(A(X), G)$ of $(A(X), F(X))$ and for every endomorphism φ of a subalgebra (B, G') of $(A(X), G)$ we have: φ is injective, $\varphi(B \cap X) \subset \subset B \cap X$, and the restriction of φ onto $B \cap X$ is increasing (i.e. if $x, y \in B \cap X$, $x < y$ then $\varphi(x) < \varphi(y)$);*

(h) *for every extension algebra $(A(X), G)$ of $(A(X), F(X))$, for every endomorphism φ of a subalgebra (B, G') of $(A(X), G)$, and for every finite subset Y of $B \cap X$ there is a unique isomorphism, namely φ, between the subalgebras of $(A(X), G)$ generated by Y and $\varphi(Y)$, respectively.*

Proof. A verification of (a) immediately follows from (f) of Lemma 10 and Construction 11. To prove (b) we note that if $x, y \in \operatorname{Im} \tau_Z$ for a finite set $Z \subset X$, then $\sigma(x, y) \in Z \cup \operatorname{Im} \tau_Z$ (by (23) and from the definition of $F'(X)$). By (22)

$\bigcup\{\mathrm{Im}\,\tau_Z;\ Z$ is a non-empty finite subset of $Y\}$ is a subalgebra of $(A(X), F(X))$. If we use (22) and (e) of Lemma 10 we see that this subalgebra is generated by Y.

To prove (c) we observe that if $z\in\mathrm{Im}\,\tau_Z$ for a finite subset Z of X then for each subalgebra (B, G) of an extension algebra $(A(X), G')$ of $(A(X), F(X))$ with $z\in B$ we have $Z\subset B$ (see (e) of Lemma 10 and (23)) and by (b) if $Z\subset B$ then $z\in B$. Condition (d) immediately follows from (b) and (c).

We prove (e). Let θ be a non-trivial congruence of an extension algebra (B, G) of a subalgebra (B, F') of $(A(X), F(X))$. We show that θ is total in the four steps that follow.

(i) If $a(\emptyset)\theta b(\emptyset)$ for some $a\neq b$, $a, b\in A$ then θ is total.
Lemma 8 implies that θ is total on $\mathrm{Im}\,\tau_\emptyset$, now by Lemma 10 θ is total on $\mathrm{Im}\,\tau_Y$ for each finite subset Y of $B\cap X$; (b) and (c) complete the proof.

(ii) If $a(\emptyset)\theta x(Y)$ for some $a\in A$, $x\in A\cup\mathrm{N}$, $\emptyset\neq Y\subset B\cap X$ then θ is total.
By (c) of Lemma 10 θ is trivial on $\mathrm{Im}\,\tau_Y$ and (i) concludes the proof.

(iii) If $n(Y)\,\theta\, m(Z)$ for $Y, Z\subset B\cap X$ with $0<\mathrm{card}\,Y<\mathrm{card}\,Z$, $n\leqq\mathrm{card}\,Y$, $m\leqq\mathrm{card}\,Z$ then θ is total.
If we use (a) of Lemma 10 we get that there are $p\neq q$, $p, q\in\mathrm{N}$ with $p(Y)\,\theta\, q(Y)$ (because $v^r(n(Y))\,\theta\, v^r(m(Z))$ for each $r\in\mathrm{N}$); now by (c) of Lemma 10 θ is total on $\mathrm{Im}\,\tau_Y$ and by (i) θ is total on B.

(iv) If $n(Y)\,\theta\, m(Z)$ for $Y, Z\subset B\cap X$ with $Z\neq Y$, $0<\mathrm{card}\,Y=\mathrm{card}\,Z$ and $n\leqq\mathrm{card}\,Y$, $m\leqq\mathrm{card}\,Z$ then θ is total.
Since $v^r(n(Y))\,\theta\, v^r(m(Z))$ for each $r\in\mathrm{N}$ we can assume that $0(Y)\,\theta\, k(Z)$ and $1(Y)\,\theta\, l(Z)$. If $l\neq 0$ then $\sigma(0(Y), l(Z))\ \theta\ \sigma(k(Z), 1(Y))$ and by (22) $\sigma(0(Y), l(Z))$, $\sigma(k(Z), 1(Y))$ are distinct elements of $\mathrm{Im}\,\tau_{Y\cup Z}$; thus θ is total on $\mathrm{Im}\,\tau_{Y\cup Z}$ by (c) of Lemma 10 and by (i) is total on B. If $l=0$ and $\mathrm{card}\,Y\geqq 2$ then $2(Y)\,\theta\, 1(Z)$ and by the same argument as above (we exchange pairs $1(Y)\,\theta\, 0(Z)$ and $2(Y)\,\theta\, 1(Z)$) we obtain that θ is total. If $l=0$ and $\mathrm{card}\,Y=1$ then $2(Y)=\sigma(0(Y), 1(Y))\,\theta\,\sigma(1(Z), 0(Z))=0(Z)\,\theta\, 1(Y)$ (we use that $\mathrm{card}\,Z=1$ implies $k=1$) hence θ is total on $\mathrm{Im}\,\tau_Y$, and θ is total by (i).

To finish the proof assume that $y(Y)\,\theta\, z(Z)$ where $y(Y)\neq z(Z)$. If $Y=Z$ then by (c) of Lemma 10 θ is total on $\mathrm{Im}\,\tau_Y$ and by (i) is total on B. If $Y\neq Z$ we note that $v^r(y(Y))\,\theta\, v^r(z(Z))$ for each $r\in\mathrm{N}$, and by (a) of Lemma 10 we obtain that the hypotheses of (iii) or (iv) are fulfilled. Thus θ is total and (B, G) is simple.

We prove (f). Let Y, Z be non-empty finite subsets of X with $\mathrm{card}\,Y=\mathrm{card}\,Z$. Then there is an order-preserving isomorphism $\psi\colon Y\to Z$ which maps the k-th element of Y onto the k-th element of Z. We shall extend ψ to an isomorphism of the subalgebras of $(A(X), F(X))$ generated by Y, Z respectively as follows: For a subset Y' of Y and for $x\in A\cup A'\cup\mathrm{N}$ we put $\psi(\tau_{Y'}(x))=\tau_{Z'}(x)$ where $Z'=\psi(Y')$. From (b) we see that ψ is a bijection of the subalgebra of $(A(X), F(X))$ generated by Y onto the subalgebra of $(A(X), F(X))$ generated by Z. A verification that it is a homomorphism is straightforward, we use (21), (22) and (23) and the definition of $F'(X)$. By the same way we get that the inverse of ψ is a homomorphism.

We prove (g). If φ is an endomorphism of a subalgebra (B, G') of an extension algebra $(A(X), G)$ of $(A(X), F(X))$ then by (e) it is one-to-one. For every $x\in B\cap X$ we have $\nu^2(x)=x$, thus $\nu^2(\varphi(x))=\varphi(x)$ and by Lemma 10 we get either $\varphi(x)\in X$ or $\varphi(x)=1(\{z\})$ for some $z\in X$. If $\varphi(x)=1(\{z\})$ then analogously as in Lemma 10, $\varphi(1(\{x\}))=z$ and $\varphi(x)=\varphi(\sigma(1(\{x\}), x))=\sigma(\varphi(1(\{x\})), \varphi(x))=\sigma(z, 1(\{z\}))= =2(\{z\})$, a contradiction (we use (9), (10) and (11)). Therefore $\varphi(x)\in X$ and thus $\varphi(B\cap X)\subset B\cap X$. Now, (21) implies that the restriction of φ to $B\cap X$ is increasing.

Condition (h) is a consequence of (g) because, by (g), φ is uniquely determined on the generating set (see (c)).

Construction 13. Let (X, φ) be an α-set pair where $\alpha\leqq\max\{2^{|\Delta|}, 2^{\aleph_0}\}$. If Y is a non-empty finite subset of X and $a, b\in A$ then $\sigma(a(\emptyset), b(Y))$ is not defined in $(A(X), F(X))$ and if $n, m\in\mathrm{N}$, $n, m>5$, $n\neq m+1$ then $\sigma(n(Y), m(Y))$ is not defined either. Choose a set $T\subset U=\{(a, b);\ a, b\in A\}\cup\{(n, m);\ n, m\in\mathrm{N},\ n, m>5,\ n\neq m, m+1\}$ with $\operatorname{card} T=\operatorname{card} U-T=\max\{|\Delta|, \aleph_0\}$. Let $(A(X), F(X, \varphi))$ be an extension algebra of $(A(X), F(X))$ such that:

(24) For each non-empty finite subset Y of X and for each pair $(u, v)\in\bigcup\{\operatorname{Im}\tau_Z;\ Z\subset Y\}$, $\sigma(u, v)$ is defined if and only if $(u, v)\notin\{(a(\emptyset), b(Z));\ (a, b)\in T,\ a, b\in A,\ \emptyset\neq Z\subset Y\}\cup\{(n(Z), m(Z));\ (n, m)\in T,\ n, m\in\mathrm{N},\ \emptyset\neq Z\subset Y\}$ and $\sigma(u, v)\in\bigcup\{\operatorname{Im}\tau_Z;\ Z\subset Y\}$;

(25) if (Y, Z) is a pair of finite subsets of X with $\operatorname{card} Y=\operatorname{card} Z$ and $\varphi(Y)\neq\varphi(Z)$ then there is a pair $(x, y)\in U-T$ such that for $x, y\in A$ if $z(Y)=\sigma(x(Y), y(\emptyset))$ then $z(Z)\neq\sigma(x(Z), y(\emptyset))$, for $x, y\in\mathrm{N}$ then $z(Y)=\sigma(x(Y), y(Y))$ implies $z(Z)\neq\sigma(x(Z), y(Z))$.

Evidently, since $\alpha\leqq\max\{2^{|\Delta|}, 2^{\aleph_0}\}$ and $\operatorname{card} U=\max\{|\Delta|, \aleph_0\}$, conditions (24) and (25) can be fulfilled.

Proposition 14. *Let (X, φ) be an α-set pair without a good sequence and $\alpha\leqq\leqq\max\{2^{|\Delta|}, 2^{\aleph_0}\}$. Then $(A(X), F(X, \varphi))$ fulfils:*

(a) *each subalgebra of $(A(X), F(X, \varphi))$ is strongly simple and strongly rigid;*

(b) *the lattice of all subalgebras of $(A(X), F(X, \varphi))$ is isomorphic to the lattice of all subsets of X;*

(c) *for every finite subset Y of X there are* $\max\{|\Delta|, \aleph_0\}$ *pairs $x, y\in\operatorname{Im}\tau_Y$ such that $\sigma(x, y)$ is not defined in $(A(X), F(X, \varphi))$;*

(d) *if (B, G) is a finitely generated subalgebra of $(A(X), F(X, \varphi))$ then $B\cap X$ is finite and generates (B, G);*

(e) *if a subalgebra (B, G) of $(A(X), F(X, \varphi))$ is generated by $Y\subset X$ then $B\cap X=Y$.*

Proof. Since for $(a, b)\in T$, $a, b\in A$, $\sigma(a(\emptyset), b(Y))$ is not defined and for $(n, m)\in T$, $n, m\in \mathbf{N}$, $\sigma(n(Y), m(Y))$ is not defined and $\operatorname{card} T=\max\{|\Delta|, \aleph_0\}$, we get (c). Condition (b) immediately follows from (d) of Proposition 12 and (24). Conditions (d) and (e) follow from (b) and (c) of Proposition 12 and (24). By (e) of Proposition 12 and by the fact that $(A(X), F(X, \varphi))$ is an extension algebra of $(A(X), F(X))$ we get that each subalgebra of $(A(X), F(X, \varphi))$ is strongly simple. To show that it is strongly rigid, let (B, G) be an extension algebra of a subalgebra (B, F') of $(A(X), F(X, \varphi))$. Evidently, there is an extension algebra $(A(X), G')$ of $(A(X), F(X))$ such that (B, G) is a subalgebra of $(A(X), G')$. Thus if ψ is an endomorphism of (B, G) then ψ is injective, $\psi(B\cap X)\subset B\cap X$ and the restriction of ψ to $B\cap X$ is increasing by (g) of Proposition 12. Since $B\cap X$ is well-ordered, we have $\psi(x)\geqq x$ for each $x\in B\cap X$. If ψ is not identical then by (c) of Proposition 12 there is $x\in B\cap X$ with $\psi(x)\neq x$. Put $x_0=x$ and define $x_{i+1}=\psi(x_i)$. Then $x_0<x_1<<x_2<\ldots$. We show that it is a good sequence with respect to (X, φ), which will be a contradiction. For a finite subset V of $\{x_0, x_1, \ldots\}$, and for each $k\in \mathbf{N}$, $\psi^k(V)==\{x_{i+k};\ x_i\in V\}$. Then by (f) and (h) of Proposition 12 $\psi(\tau_V(x))=\tau_{\psi(V)}(x)$ for each $x\in A_n$ where $\operatorname{card} V=n$. Hence for each $(a, b)\in U-T$ if $\sigma(a(V), b(\emptyset))=x(V)$ and $a, b\in A$ then $\sigma(a(\psi(V)), b(\emptyset))=x(\psi(V))$, if $\sigma(a(V), b(V))=x(V)$ and $a, b\in \mathbf{N}$ then $\sigma(a(\psi(V)), b(\psi(V)))=x(\psi(V))$ and so $\varphi(V)=\varphi(\psi(V))==\varphi(\psi^k(V))$ for each $k\in \mathbf{N}$ (see (25)). Thus $\{x_0, x_1, \ldots\}$ is a good sequence, a contradiction. Hence ψ is the identity and (a) holds.

Proof of Theorem 1. We are to show (a)⇒(c). By the definition of $\operatorname{Set}(\alpha)$, however, there is an α-set pair (X, φ) without a good sequence with $\operatorname{card} X\geqq\beta$. Furthermore, $\operatorname{card} A(X)\geqq\operatorname{card} X$; Lemma 5 and Proposition 14 now complete the proof.

Proof of Theorem 3. Let L be an algebraic lattice such that for $\alpha==\max\{|\Delta|, \aleph_0\}$, $2^\alpha>d(L)$, $\alpha\geqq c(L)$. Let C be the set of all compact elements of L. Since $2^\alpha>d(L)$ there is an 2^α-set pair (C, φ) without a good sequence. Consider a partial algebra $(A(C), F(C, \varphi))$ from Proposition 14. Let $(A(C), F(L))$ be an extension algebra of $(A(C), F(C, \varphi))$ such that:

(26) for each pair $c, d\in C$ with $c<d$ there is $(x, y)\in T$ such that if $x, y\in A$ then $\sigma(x(\emptyset), y(\{c\}))=d$, if $x, y\in \mathbf{N}$ then $\sigma(x(\{c\}), y(\{c\}))=d$;

(27) for each finite subset Y of C there is $(x, y)\in T$ such that if $x, y\in A$ then $\sigma(x(\emptyset), y(Y))=c=\vee Y$, if $x, y\in \mathbf{N}$ then $\sigma(x(Y), y(Y))=c=\vee Y$;

(28) for the other pairs $x, y\in A(C)$ such that $\sigma(x, y)$ is not defined, set $\sigma(x, y)=x$.

By (a) of Proposition 14 and by Proposition 5 each subalgebra is simple and rigid, moreover $(A(C), F(L))$ is a total algebra by (28). By (d) of Proposition 14 and by

(27) and (28) each finitely generated subalgebra of $(A(C), F(L))$ is generated by some $\{c\}$, $c\in C$ or by $\emptyset$. Moreover by (c) of Proposition 14 and by (26), (27) and (28) $c\leqq d$ in C iff the subalgebra of $(A(C), F(L))$ generated by $\{c\}$ is contained in the subalgebra of $(A(C), F(L))$ generated by $\{d\}$. By (e) of Proposition 14 the lattice of all subalgebras of $(A(C), F(L))$ is isomoiphic to L. Conversely, if (A, F) is an algebra of type Δ such that each subalgebra of (A, F) is rigid and simple and the lattice of all subalgebras of (A, F) is isomorphic to L then by Theorem 1, $2^{\alpha}>d(L)$ where $\alpha=\max\{|\Delta|, \aleph_0\}$. Further, each finitely generated subalgebra (B, G) of (A, F) fulfils card $B\leqq\alpha$ and thus it has at most α finitely generated subalgebras. Thus $c(L)\leqq\alpha$ and Theorem 3 is proved.

Proof of Corollary 2. Let Δ be an infinitary type. Analogously to Lemma 6 we see that in the proof of Corollary 2 we may assume that Δ contains one ω_0-ary operation ω. Let $\Delta'=\{\sigma\}$ be a type where σ is binary, let (X, φ) be an $\aleph_0$-set pair and let $(A(X), F(X, \varphi))$ be a partial algebra from Construction 13 of type Δ'. Define a partial algebra $(A(X), G(X, \varphi))$ of type Δ: choose a mapping η from the set of all increasing sequences in X onto $\{0, 1\}$ such that $\eta(\{x_0, x_1, ...\})\neq\eta(\{x_1, x_2, ...\})$ for each increasing sequence $\{x_0<x_1<...\}$ in X (see [7]),

$$\omega(\{x_0, x_1, ...\}) = \sigma(x_0, x_1) \quad \text{if} \quad \{x_0, x_1, ...\} \tag{29}$$

is not one-to-one and $\sigma(x_0, x_1)$ is defined,

$$\omega(\{x_0, x_1, ...\}) = x_{\eta(\{x_0, x_1, ...\})} \quad \text{if} \quad \{x_0, x_1, ...\} \tag{30}$$

is an increasing sequence of elements in X.

Then each subalgebra of $(A(X), G(X, \varphi))$ is strongly simple and strongly rigid. If (B, G) is an extension algebra of a subalgebra (B, G') of $(A(X), G(X, \varphi))$ then there is F' such that (B, F') is a subalgebra of $(A(X), F(X, \varphi))$ and each congruence θ on (B, G) is a congruence on (B, F'); hence (B, G) is simple. Each endomorphism ψ of (B, G) is also an endomorphism of (B, F') thus by (g) of Proposition 12 ψ is injective, $\psi(B\cap X)\subset B\cap X$ and ψ is increasing on $B\cap X$. Thus $\psi(x)\geqq x$ for each $x\in B\cap X$. If ψ is not identical, then by (c) of Proposition 12 there is an $x\in B\cap X$ with $\psi(x)\neq x$. Now we define an increasing sequence $x_0=x$, $x_{i+1}=\psi(x_i)$ in $B\cap X$. By an easy calculation (see [7])

$$\psi(\omega(x_0, x_1, ...)) \neq \omega(\psi(x_0), \psi(x_1), ...) = \omega(x_1, x_2, ...),$$

a contradiction. Hence (B, G) is rigid. Now Proposition 5 concludes the proof.

Sketch of the proof of Theorem 4. Assume that L is an m-algebraic lattice and Δ is an infinitary type such that there is an algebra (A, F) of type Δ such that each of its subalgebras is simple and rigid, and the lattice of all subalgebras of (A, F) is isomorphic to L. It is well known that $m\leqq\sup\Delta$. Since m-compact elements correspond to subalgebras of (A, F) generated by a set of power less than m and because for each subalgebra (B, F') of (A, F) generated by a set of power less than m we have $\operatorname{card} B \leqq |\Delta| \cdot 2^{\alpha}$ where $\alpha < \sup \Delta$, we get that $c_m(L) \leqq |\Delta| \cdot 2^{n\alpha}$ for $n < m$, $\alpha < \sup \Delta$. Conversely, let L be an m-algebraic lattice and Δ be a type such that $m \leqq \sup \Delta$ and $c_m(L) \leqq |\Delta| \cdot 2^{n\alpha}$. We can assume that Δ contains a nullary operation symbol. It is routine to prove the following modification of Construction 7 and Lemma 8: *There is a simple algebra (A, F) of type Δ generated by $\emptyset$ such that* $\operatorname{card} A \geqq c_m(L)$ *and for an infinitary operation symbol $\sigma \in \Delta$ if we set $v(a) = \sigma(a, a, \ldots)$ then for each $a \in A$, $n \in \mathrm{N}$, $n \neq 0$, $v^n(a) \neq a$.* Now, if we substitute this algebra (A, F) into the construction of $(A(X), G(X, \varphi))$ described in the proof of Corollary 2, we obtain the existence of a partial algebra (B, G) of type Δ containing the set L' of all m-compact elements of L and such that:

(a) each subalgebra of (B, G) is strongly simple and strongly rigid;

(b) each subalgebra (C, G') of (B, G) is generated by $C \cap L'$;

(c) for each subset C of L', if (C', G') is a subalgebra of (B, G) generated by C then $C' \cap L' = C$;

(d) if a subalgebra (C, G') of (B, G) is generated by a set of power less than m then $\operatorname{card} C \cap L' < m$;

(e) for each subset C of L', $\operatorname{card} C < m$, if (C', G') is a subalgebra of (B, G) generated by C then there are at least $c_m(L)$ sequences τ, $\{x_i;\ i \in \operatorname{ar} \tau\}$ such that $\tau \in \Delta$, $x_i \in C'$ for $i \in \operatorname{ar} \tau$ and $\tau(\{x_i;\ i \in \operatorname{ar} \tau\})$ is not defined.

Arguments identical to those used in the proof of Theorem 3 show that there is an algebra of type Δ with the required properties.

We can observe that in the proof of Theorem 3 there are at least $\max\{|\Delta|, \aleph_0\}$ pairs such that $\sigma(x, y)$ is defined by (28), i.e. $\sigma(x, y) = x$. If we redefine a set of such pairs x, y such that $\sigma(x, y) = y$ then the required properties of algebra do not change — but two distinct such extension algebras are mutually rigid. Analogous consideration can be used for the proof of Theorem 4. We obtain:

Corollary 15. *Let m be a regular cardinal, L' the set of all m-compact elements of an m-algebraic lattice L. If Δ is a non-unary type such that $\sup \Delta \geqq m$ or $m = \aleph_0$ and $d(L) < \max\{2^{|\Delta|}, 2^{\aleph_0}\}$ and $c_m(L) \leqq |\Delta| \cdot \aleph_0^{n\alpha}$ where $n < m$, $\alpha < \sup \Delta$ in either case, then on a set of cardinality $\beta = \operatorname{card} L' \cdot |\Delta| \cdot \aleph_0^{\alpha}$ where $\alpha < \sup \Delta$ there are $\sup\{\beta^{\alpha};\ \alpha < \sup \Delta\}$ algebras of type Δ such that:*

(a) *each subalgebra of each algebra is rigid and simple;*

(b) *the lattice of all subalgebras of each algebra is isomorphic to L;*

(c) *each pair of algebras is mutually rigid.*

References

[1] M. AMBRUST, J. SCHMIDT, Zum Cayleyschen Darstellungssatz, *Math. Ann.*, **154** (1964), 70—72.

[2] G. BIRKHOFF, O. FRINK, Representations of lattices by sets, *Trans. Amer. Math. Soc.*, **64** (1948), 299—316.

[3] E. FRIED, J. SICHLER, On automorphism groups of subalgebras of universal algebra, *Acta Sci. Math.*, **40** (1978), 265—271.

[4] G. GRÄTZER, *Universal Algebra*, Second Edition, Springer-Verlag (Berlin—New York—Heidelberg, 1979).

[5] G. GRÄTZER, E. T. SCHMIDT, Characterization of congruence lattices of abstract algebras, *Acta Sci. Math.*, **24** (1963), 34—59.

[6] J. KOLLÁR, Automorphism groups of subalgebras; a concrete characterization, *Acta Sci. Math.*, **40** (1978), 291—295.

[7] V. KOUBEK, V. RÖDL, On combinatorial properties of universal algebras, to appear.

[8] W. A. LAMPE, The independence of certain related structures of a universal algebra, *Algebra Universalis*, **2** (1972), Part I, 99—112; Part II, 270—283; Part III, 286—295; Part IV, 296—302.

[9] N. SAUER, M. G. STONE, Endomorphism and subalgebra structure; a concrete characterization, *Acta Sci. Math.*, **39** (1977), 397—402.

COMPUTATIONAL CENTRE OF CHARLES UNIVERSITY
MALOSTRANSKÉ NÁM. 25
118 00 PRAHA 1, CZECHOSLOVAKIA